janet

Using data from pastebin.com for incident response and investigation.

Lee Harrigan

Why did we start to monitor pastebin.com?

janet

50 Days of Lulz

BY: A GUEST ON JUN 25TH, 2011 | SYNTAX: NONE | SIZE: 4.71 KB | HITS: 424,061 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE

```
. /$$                /$$            /$$$$$$
.| $$               | $$           /$$__  $$
.| $$       /$$   /$$| $$ /$$$$$$$$| $$  \__/  /$$$$$$   /$$$$$$$
.| $$      | $$  | $$| $$|____ /$$/| $$$$$$  /$$__  $$ /$$_____/
.| $$      | $$  | $$| $$   /$$$$/  \____  $$| $$$$$$$$| $$
.| $$      | $$  | $$| $$  /$$__/   /$$  \ $$| $$_____/| $$
.| $$$$$$$$|  $$$$$$/| $$ /$$$$$$$$|  $$$$$$/|  $$$$$$$|  $$$$$$.$
.|________/ \______/ |__/|________/ \______/  \_______/ \_______/
                          //Laughing at your security since 2011!

.--    .-""-.
.   ) (     )
.  (   )   (
.     /     )
.    (_    _)                    0_,-.__
.      (_  )_                    |_.-._/
.       (    )                   |lulz..\
.        (__)                    |__--_/
.     |''   ``\                  |
.     | [Lulz] \                 |      /b/
.     |         \  ,,,---===?A`\  |  ,==y'
.   ___,,,,,---==""\         |M] \ | ;|\ |>
.          _   _   \   ___,|H,,---=="""""bno,
.    o  O  (_) (_)   \ /          _     AWAW/
.                     /         _(+)_  dMM/
.      \@_,,,,,,---=="   \      \\|//  MW/
.--''''"                         ===  d/
.                                   //   SET SAIL FOR FAIL!
.                                    ,'_____________________
.   \    \    \     \               ,/~~~~~~~~~~~~~~~~~~~~~~~~~~
.                          _____    ,'  ~~~   .-""-.~~~~~~  .-""-.
.      .-""-.           ///==---   /`-._ ..-'      -.__..-'
.            `-.__..-' =====\\\\\\ V/  .---\.
.                     ~~~~~~~~~~~, _',--/_.\  .-""-.
.                             .-""-.___` --  \|         -.__..-

Friends around the globe,
```

Anonymous

@YourAnonNews

Follow

Happy #LulzXmas | @STRATFOR database dump + 30,000 cc/ccv #s -- pastebin.com/q5kXd7Fd | #Anonymous #AntiSec #LulzSec #ExpectUs

Reply Retweet Favorite

antisec teaser 12/26

BY: A GUEST ON DEC 26TH, 2011 | SYNTAX: NONE | SIZE: 6.36 KB | HITS: 30,

DOWNLOAD | RAW | EMBED | REPORT ABUSE

```
  _____
 /     \   _____________________ ___.__.
/  \ /  \_/ __ \_  __ \_  __ <   |  |
\   Y    \  ___/|  | \/|  | \/\___  |
 \____|__  /\___  |__|   |__|   / ____|
         \/     \/              \/

.____          .__         ____  ___
|    |    __ __|  | _______\   \/  / _____ _____    ______
|    |   |  |  |  | \___   /\     / /     \\__  \  /  ___/
|    |___|  |  |  |__/    / /     \|  Y Y  \/ __ \_\___ \
|_______ |____/|____/_____ /___/\  |__|_|  (____  /____  >
        \/                \/     \_/     \/     \/     \/
```

Why did we start to monitor pastebin.com?

janet

- Increasing amount of breached data being dumped onto pastebin.com
- We know people reuse passwords, no matter how much we tell them not to!
- Stratfor hack was announced on December 26th 2011 while we were operating a reduced level of service.
- The team were not aware about the Stratfor hack until January 3rd when back to normal operation.
- Compromised sites details notified on the 4th of January (9 days after the hack)
- Potential damage could have been widespread for you.
- We deemed the delay was too long and something needed to be done.

All good ideas stem from others attempts

janet

On the 16th of January we saw the following tweet

Problems with the tweeted code

janet

- The perl version was rather simple and effectively DOS'd pastebin.com with requests.
- Would report on a match of a single term. This would generate a lot of reports if we just searched for "ac.uk" or "hacked" or "sqli"
- Pastes were being missed due to too many requests to and not checking for timeouts.
- Only URL's were logged so if pastes were taken down or expired there was no way to verify the incident.
- Would track every paste ever checked causing a very large text file to be checked against every new paste causing a greater delay.

How do we do it!

janet

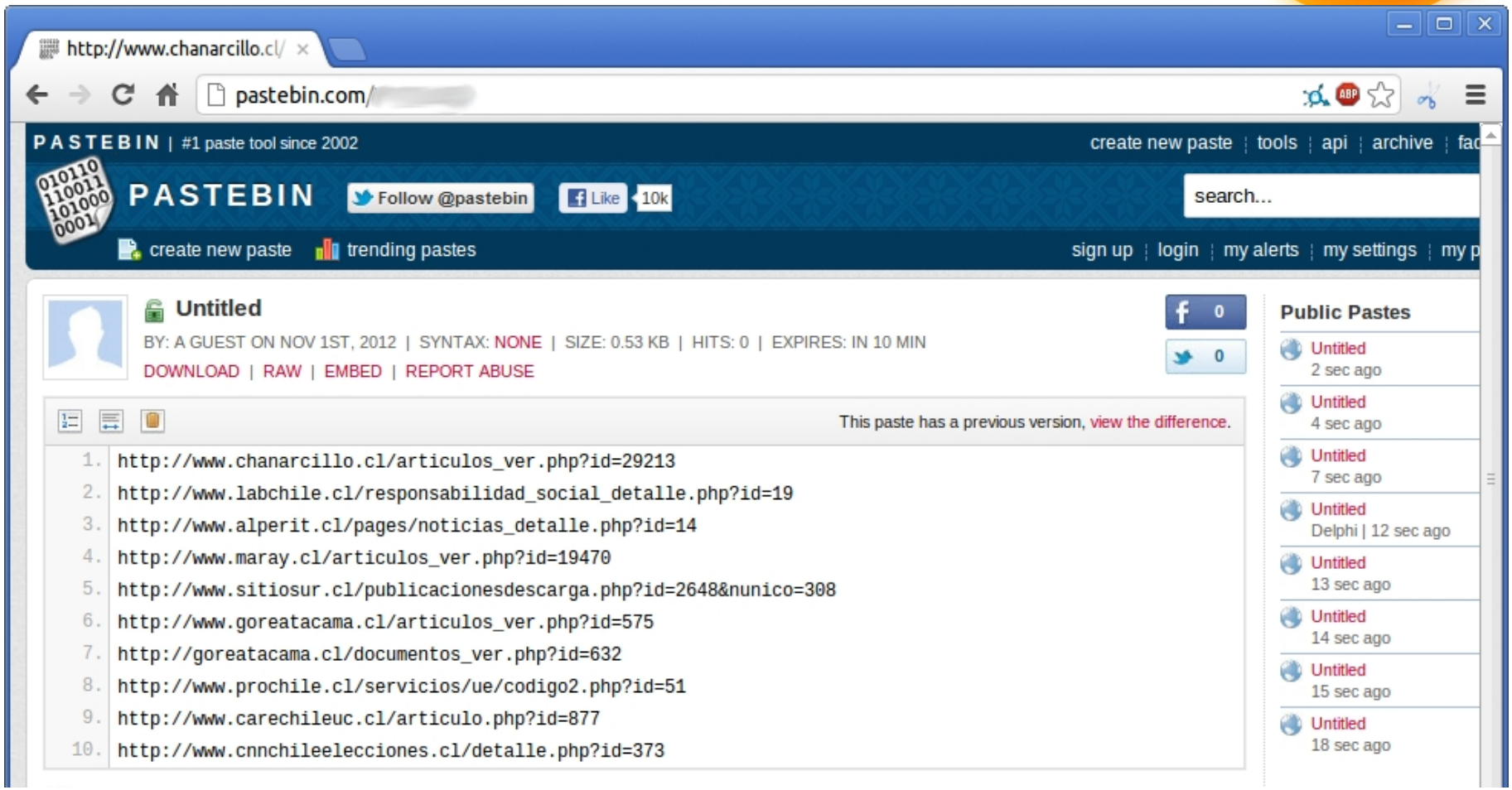
- Python > Perl ☺
- Look for a combination of Domains or ASN 786 IP address & keywords within a single paste. eg '.ac.uk ' and 'dos' or '193.x.x.x' and 'sql injection'
- HTTP Request flow control so we do not spam requests to pastebin.
- HTTP timeout detection.
- Implement a track of the last pastes checked so we don't check the same paste several times.
- Keep a record of previous raised pastes and check each new report against old pastes to see if the data is old.
- Keep a local copy of reported pastes so we can search through and see if a new paste is just old data posted again.

So what types of reports do we see!

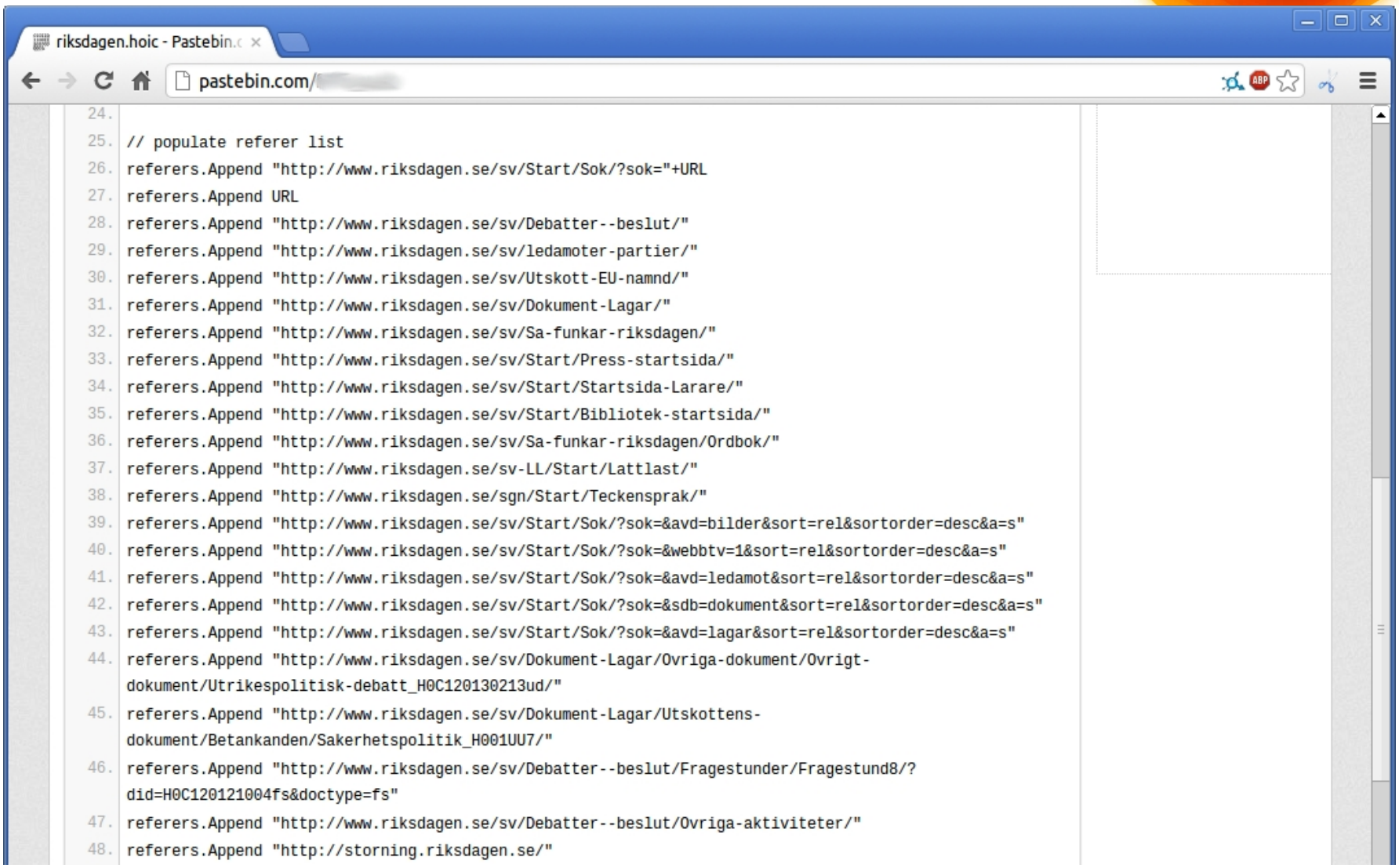
janet

- SQL Injection vulnerable URL's
- DDOS Targets
- Compromised data dumps (Username / password / Hash)
- System configuration files / Application code
- Intelligence gathering (Nessus / Nmap scan results)
- Open proxies
- Cyber graffiti (Insecure Wiki's)
- IRC chat logs
- Credit card information
- Personal information

SQL Injection URL's



HOIC DDOS Configuration files

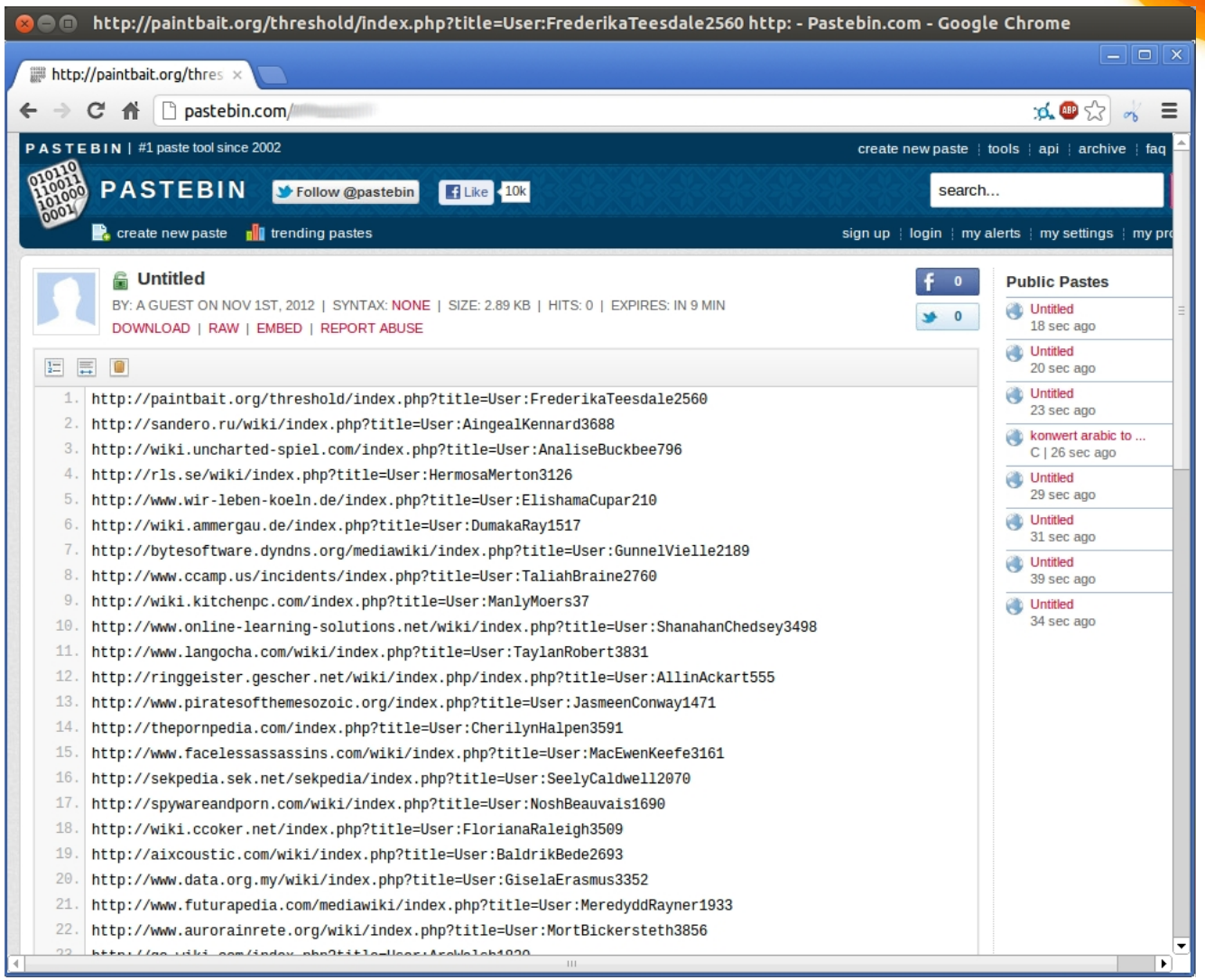



```
24.
25. // populate referer list
26. referers.Append "http://www.riksdagen.se/sv/Start/Sok/?sok="+URL
27. referers.Append URL
28. referers.Append "http://www.riksdagen.se/sv/Debatter--beslut/"
29. referers.Append "http://www.riksdagen.se/sv/ledamoter-partier/"
30. referers.Append "http://www.riksdagen.se/sv/Utskott-EU-namnd/"
31. referers.Append "http://www.riksdagen.se/sv/Dokument-Lagar/"
32. referers.Append "http://www.riksdagen.se/sv/Sa-funkar-riksdagen/"
33. referers.Append "http://www.riksdagen.se/sv/Start/Press-startsida/"
34. referers.Append "http://www.riksdagen.se/sv/Start/Startsida-Larare/"
35. referers.Append "http://www.riksdagen.se/sv/Start/Bibliotek-startsida/"
36. referers.Append "http://www.riksdagen.se/sv/Sa-funkar-riksdagen/Ordbok/"
37. referers.Append "http://www.riksdagen.se/sv-LL/Start/Lattlast/"
38. referers.Append "http://www.riksdagen.se/sgn/Start/Teckensprak/"
39. referers.Append "http://www.riksdagen.se/sv/Start/Sok/?sok=&avd=bilder&sort=rel&sortorder=desc&a=s"
40. referers.Append "http://www.riksdagen.se/sv/Start/Sok/?sok=&webbtv=1&sort=rel&sortorder=desc&a=s"
41. referers.Append "http://www.riksdagen.se/sv/Start/Sok/?sok=&avd=ledamot&sort=rel&sortorder=desc&a=s"
42. referers.Append "http://www.riksdagen.se/sv/Start/Sok/?sok=&sdb=dokument&sort=rel&sortorder=desc&a=s"
43. referers.Append "http://www.riksdagen.se/sv/Start/Sok/?sok=&avd=lagar&sort=rel&sortorder=desc&a=s"
44. referers.Append "http://www.riksdagen.se/sv/Dokument-Lagar/Ovriga-dokument/Ovrigt-
    dokument/Utrikespolitisk-debatt_H0C120130213ud/"
45. referers.Append "http://www.riksdagen.se/sv/Dokument-Lagar/Utskottens-
    dokument/Betankanden/Sakerhetspolitik_H001UU7/"
46. referers.Append "http://www.riksdagen.se/sv/Debatter--beslut/Fragestunder/Fragestund8/?
    did=H0C120121004fs&doctype=fs"
47. referers.Append "http://www.riksdagen.se/sv/Debatter--beslut/Ovriga-aktiviteter/"
48. referers.Append "http://storning.riksdagen.se/"
```

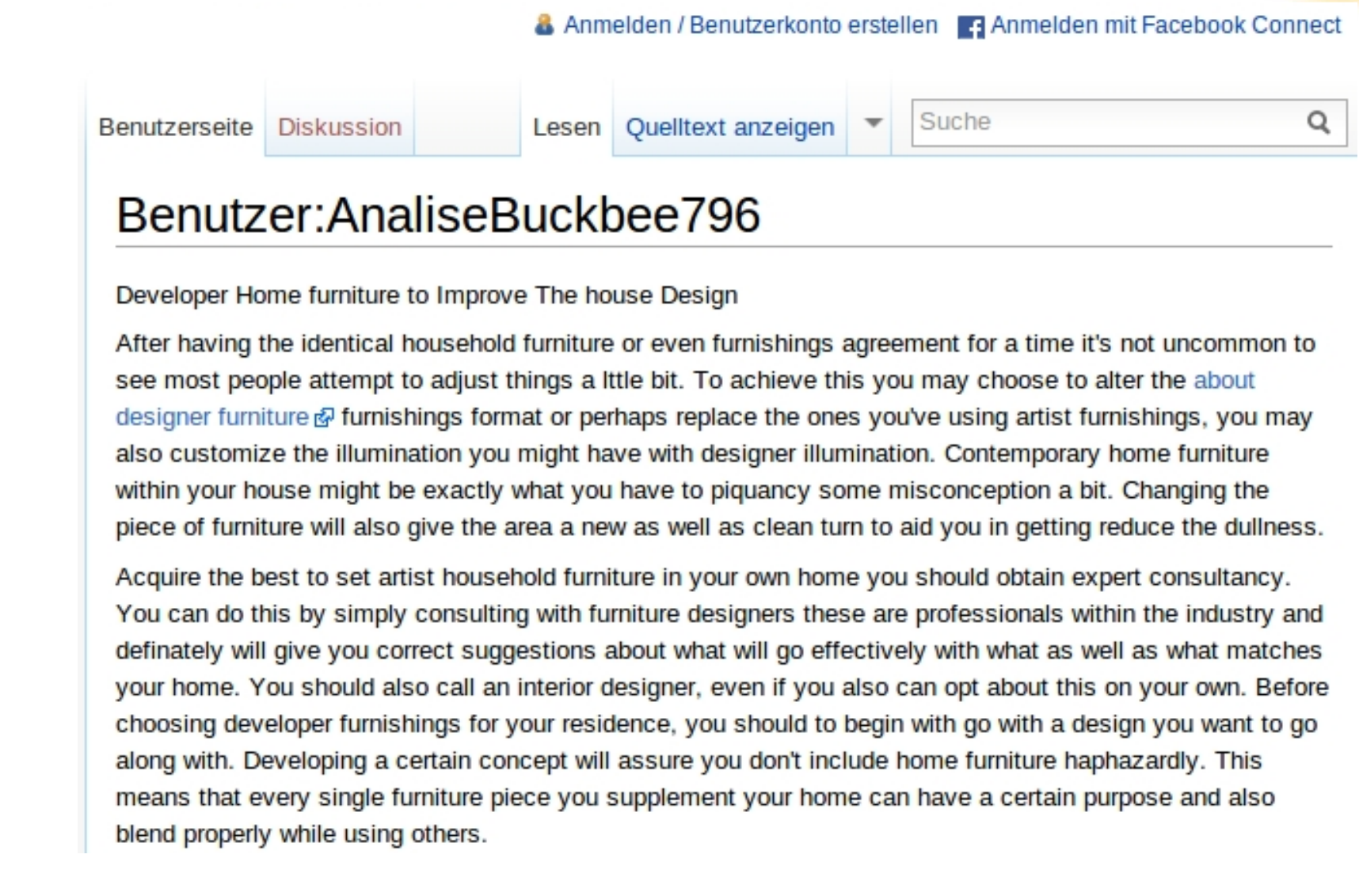
Code sample

janet

Cyber graffiti (Insecure Wiki's)



Cyber graffiti (Insecure Wiki's)



Anmelden / Benutzerkonto erstellen Anmelden mit Facebook Connect

Benutzerseite | Diskussion | Lesen | Quelltext anzeigen | Suche

Benutzer:AnaliseBuckbee796

Developer Home furniture to Improve The house Design

After having the identical household furniture or even furnishings agreement for a time it's not uncommon to see most people attempt to adjust things a lttle bit. To achieve this you may choose to alter the about designer furniture furnishings format or perhaps replace the ones you've using artist furnishings, you may also customize the illumination you might have with designer illumination. Contemporary home furniture within your house might be exactly what you have to piquancy some misconception a bit. Changing the piece of furniture will also give the area a new as well as clean turn to aid you in getting reduce the dullness.

Acquire the best to set artist household furniture in your own home you should obtain expert consultancy. You can do this by simply consulting with furniture designers these are professionals within the industry and definately will give you correct suggestions about what will go effectively with what as well as what matches your home. You should also call an interior designer, even if you also can opt about this on your own. Before choosing developer furnishings for your residence, you should to begin with go with a design you want to go along with. Developing a certain concept will assure you don't include home furniture haphazardly. This means that every single furniture piece you supplement your home can have a certain purpose and also blend properly while using others.

Example 1 (Online site hacked)

janet

- A small website online was vulnerable to a SQLi attack and contents were put onto pastebin.
- Details of usernames, passwords, and email addresses were dumped.
- Automated email received at 23:15.
- By 9:30 the following morning we had sent notifications to 42 different sites about the breach.
- We also alerted the site that was hacked, they were not aware and took the site offline and also notified all users in their database about the breach.

Example 2 (Moodle System Hack)

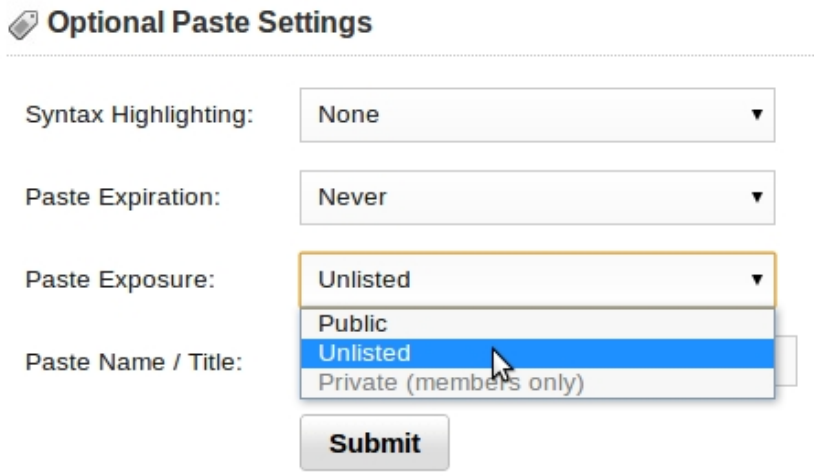
janet

- Dump detected at 21:30
- Content of usernames and hashed passwords were put on pastebin approx 3500 unique hashes.
- Investigation started at 08:50 the following day
- A Janet connected organisation system was compromised due to running a old version of phpMyAdmin on a production Moodle server.
- 48% of the passwords were cracked using a small rainbow table (lowercase alpha numeric 1-8)
- Site advised of the very weak passwords.
- They rebuilt system with salted hashing, minimum password requirements and without phpMyAdmin.
- A student at the site was responsible

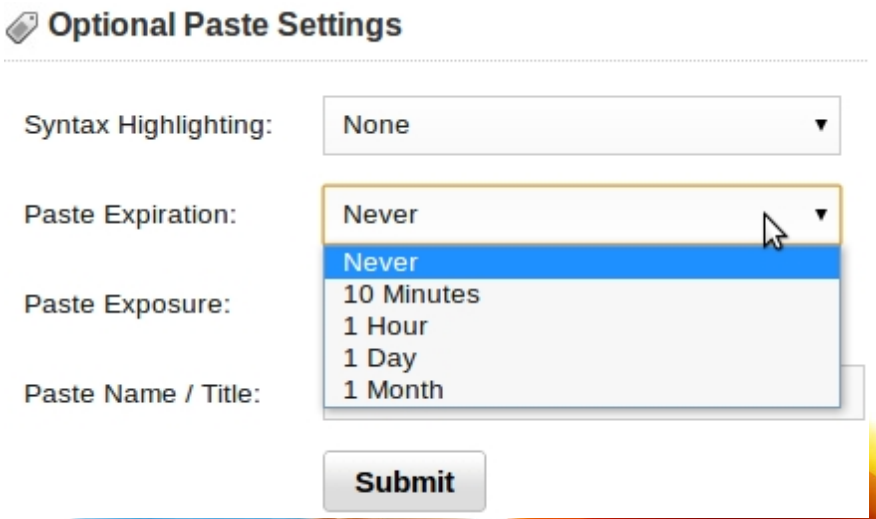
How can you use pastebin safely

janet

- Ensure that your pastes are unlisted or private pastes



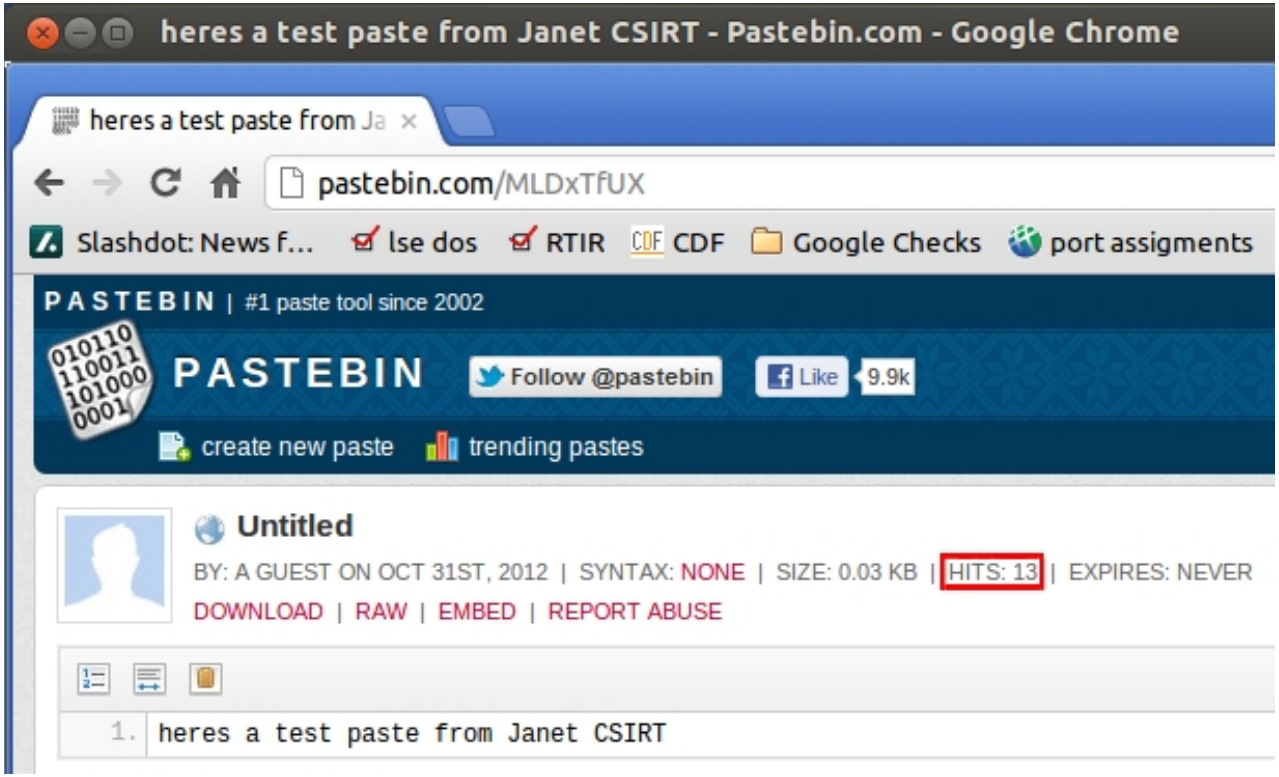
- Set a short timeout on pastes



How can you use pastebin safely

janet

- Do not paste sensitive information.



- Within 5 minutes we saw this paste as did 12 others.

Some stats (since January 1st 2012)

janet

- On average we detect ~ 7 pastes a day that we believe may warrant further investigation.
- We currently reject 82% of reports that we see. It's better to have a high rejection rate rather than miss some information.
- Over 1025 Investigations have been opened as a result of pastebin data.

Why should you worry about pastebin data?

janet

- Where user credentials are breached they may be able to use them to gain access to your systems!
  This is why we report all new incidents that we detect.
- It only takes data to be available for < 5 mins in a public paste and we will have seen it. Who are the other 12?
- Media attention can gather very quickly, you should be able to confirm or deny the information.
- Able to see if an attack is planned for your site and take actions prior.
- If we see lots of intelligence gathering for a specific site you may be attacked from the inside, where security monitoring could be less effective.

Summary / Discussion

janet

- With attacks to sites increasing recently this is a key way for us to identify Incidents ASAP.
- We offer this as part of our CSIRT service.
- Some connected sites have been contacted by third parties stating that they have obtained some account information from pastebin and would like to chat.
- Would you like to see customised searches specific to your sites, sent directly to you?
- Any questions?

janet

THANK YOU

Janet, Lumen House
Library Avenue, Harwell Oxford
Didcot, Oxfordshire
t: 0300 999 2340
e: irt@csirt.ja.net